EP 27584 (4)

EUROPEAN PATENT OFFICE

Patent Abstracts of Japan

PUBLICATION NUMBER : 11098487
PUBLICATION DATE : 09-04-99

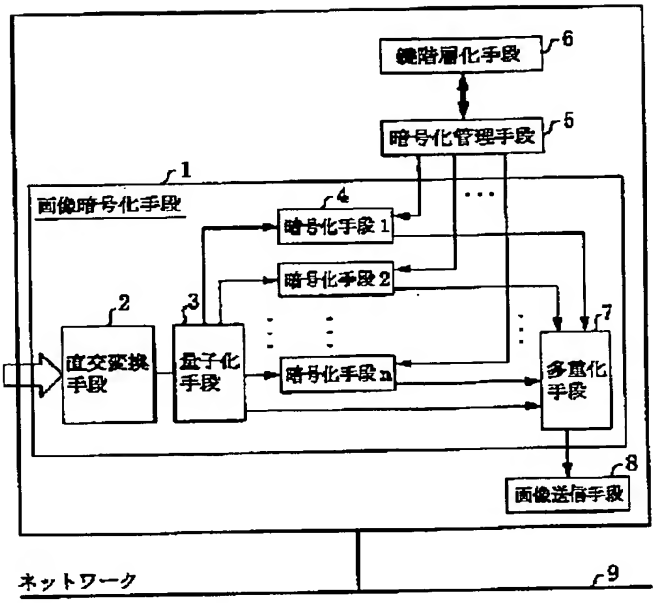
APPLICATION DATE : 24-09-97
APPLICATION NUMBER : 09258411

APPLICANT : MITSUBISHI ELECTRIC CORP;

INVENTOR : KAWACHI KIYOTO;

INT.CL. : H04N 7/167 H04N 7/30

TITLE : IMAGE CODER AND IMAGE DECODER



ABSTRACT : PROBLEM TO BE SOLVED: To select a key encryption and decoding depending on an image by dividing a quantized image into pluralities of blocks for each prescribed frequency region, using a reference key of the encryption key to generate pluralities of hierarchical encryption keys, using a quantization means to generate divided blocks and encrypting the blocks through the use of an encryption key of a prescribed hierarchical level.

SOLUTION: An encryption management means 5 generates a reference key based on a random number, a key hierarchical pressing means 6 converts the reference key to generate encryption keys to be set to each of encryption processing means 4(1-n). In a key series, a low-order key is easily generated from a high-order key and estimate of the high-order key from the low-order key is quantitatively difficult. An orthogonal transform means 2 transforms the key into a spatial frequency component, a quantization means 3 quantizes the component, divided into a predetermined spatial frequency area block, encryption is conducted by an encryption processing means 4 corresponding to respective blocks, and image information is sent to an image decoder via an image transmission means 8 and a network 9.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－98487

(43)公開日　平成11年(1999)４月９日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｎ　7/167		Ｈ０４Ｎ　7/167	Ｚ
7/30		7/133	Ｚ

審査請求　未請求　請求項の数16　ＯＬ　（全 23 頁）

(21)出願番号　特願平9－258411

(22)出願日　平成９年(1997)９月24日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　河内　清人
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

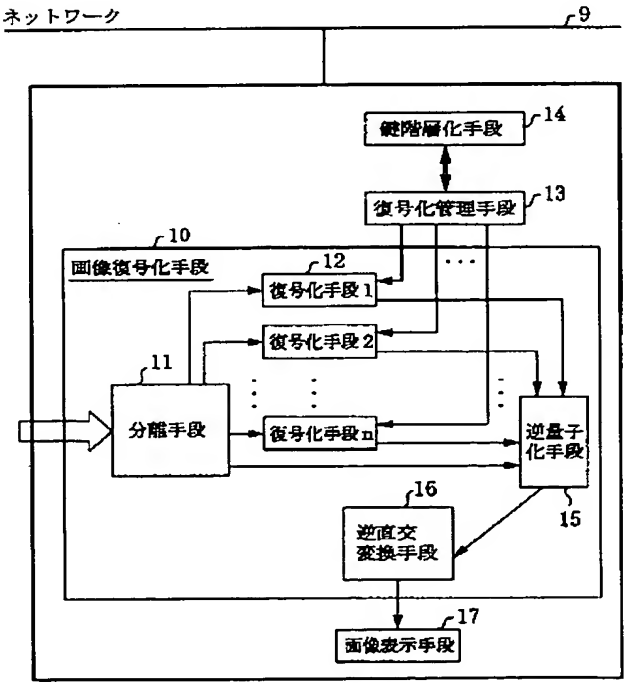
(74)代理人　弁理士　宮田　金雄　（外２名）

(54)【発明の名称】　画像符号化装置及び画像復号化装置

(57)【要約】

【課題】　画像を暗号化して提供する画像符号化装置及び画像復号化装置において、配送しなければならない鍵を一つにし、さらに異なるクラス階層を持った画像の送受信を可能にし、画像に応じて、暗号化、復号化に使用する鍵を選択可能にすることを目的とする。

【解決手段】　暗号化に使用する暗号鍵の基準となる基準鍵を用い、階層化された複数の暗号鍵を生成し、この階層レベルの暗号鍵を用いて暗号化する画像復号化装置と復号化に使用する復号鍵の基準となる基準鍵を用い、階層化された複数の復号鍵を生成し、この階層レベルの復号鍵を用いて復号化する画像復号化装置から構成したものである。



【特許請求の範囲】
【請求項１】　画像を空間周波数成分に変換する直交変換手段と、
この変換された空間周波数成分を量子化し、所定の周波数領域毎の複数のブロックに分割する量子化手段と、
暗号化に使用する暗号鍵の基準となる基準鍵を用い、階層化された複数の暗号鍵を生成する鍵階層化手段と、
前記量子化手段により分割されたブロックを、前記鍵階層化手段により生成された所定の階層レベルの暗号鍵を用いて暗号化する画像暗号化手段とを備えたことを特徴とする画像符号化装置。
【請求項２】　前記画像暗号化手段は、前記量子化手段により分割された複数のブロックをそれぞれ並列に暗号化する複数の暗号化手段と、
この複数の暗号化手段により暗号化された複数のブロックを一つにまとめる多重化手段とを備えたことを特徴とする請求項１記載の画像符号化装置。
【請求項３】　前記鍵階層化手段は、前記階層化された複数の暗号鍵を、上位の鍵から下位の鍵を得ることができる一方向性関数により生成することを特徴とする請求項１記載の画像符号化装置。
【請求項４】　前記鍵階層化手段は、前記階層化された複数の暗号鍵を、公開鍵暗号アルゴリズムにおける公開鍵を用いた暗号化により生成することを特徴とする請求項１記載の画像符号化装置。
【請求項５】　前記量子化手段は、前記量子化された空間周波数成分を、予め設定された周波数領域分割指定に基づいて複数のブロックに分割することを特徴とする請求項１記載の画像符号化装置。
【請求項６】　前記量子化手段により分割された各ブロックに関する情報を、前記画像暗号化手段により暗号化されたブロックに付加する暗号化情報付加手段を備えたことを特徴とする請求項１記載の画像符号化装置。
【請求項７】　前記暗号化情報付加手段は、周波数が最も高い領域のブロックを暗号化するために用いた暗号鍵の階層レベルを付加することを特徴とする請求項６記載の画像符号化装置。
【請求項８】　乱数の発生により新しい基準鍵を生成する新規鍵生成手段と、
この新規鍵生成手段により生成された新しい基準鍵を、この基準鍵を識別する鍵識別子とともに格納する鍵保存手段とを備え、
前記鍵階層化手段は、前記新規鍵生成手段により生成された新しい基準鍵又は前記鍵保存手段に格納されている基準鍵のいずれかを用いて、前記階層化された複数の暗号鍵を生成することを特徴とする請求項１記載の画像符号化装置。
【請求項９】　ネットワークを通じて送信されてきた所定の階層レベルの鍵要求を受信する鍵要求受信手段と、
この要求された階層レベルの暗号鍵の基準となる基準鍵を、前記新規鍵生成手段により生成するか、あるいは前記鍵保存手段より取り出し、前記要求された階層レベルの暗号鍵を前記鍵階層化手段により生成する鍵取得手段と、
この生成された暗号鍵を前記鍵要求の送信元に送信する鍵送信手段とを備えたことを特徴とする請求項８記載の画像符号化装置。
【請求項１０】　空間周波数成分に変換された画像を量子化し、暗号化して伝送された画像情報を所定の周波数領域毎の複数のブロックに分割する分離手段と、
復号化に使用する復号鍵の基準となる基準鍵を用い、階層化された複数の復号鍵を生成する復号鍵階層化手段と、
前記分離手段により分割されたブロックを、前記復号鍵階層化手段により生成された所定の階層レベルの復号鍵を用いて復号化する画像復号化手段とを備えたことを特徴とする画像復号化装置。
【請求項１１】　前記画像復号化手段は、前記分離手段により分割された複数のブロックをそれぞれ並列に復号化する複数の復号化手段と、
この複数の復号化手段により復号化された複数のブロックを逆量子化し、空間周波数成分に変換する逆量子化手段と、
この逆量子化手段により変換された空間周波数成分を元の画像に変換する逆直交変換手段とを備えたことを特徴とする請求項１０記載の画像復号化装置。
【請求項１２】　前記復号鍵階層化手段は、前記階層化された複数の復号鍵を、上位の鍵から下位の鍵を得ることができる一方向性関数により生成することを特徴とする請求項１０記載の画像復号化装置。
【請求項１３】　前記復号鍵階層化手段は、前記階層化された複数の復号鍵を、公開鍵暗号アルゴリズムにおける公開鍵を用いた暗号化により生成することを特徴とする請求項１０記載の画像復号化装置。
【請求項１４】　前記分離手段は、予め設定された周波数領域分割指定に基づいて複数のブロックに分割することを特徴とする請求項１０記載の画像復号化装置。
【請求項１５】　外部から新しい基準鍵を入力する鍵入力手段と、この基準鍵を基準鍵識別子とともに格納する鍵保存手段とを備え、
前記復号鍵階層化手段は、前記鍵入力手段により入力された新しい基準鍵又は前記鍵保存手段に格納されている基準鍵のいずれかを用いて、前記階層化された複数の復号鍵を生成することを特徴とする請求項１０記載の画像復号化装置。
【請求項１６】　前記鍵保存手段は、基準鍵識別子に加えて鍵生成者の識別子を格納することを特徴とする請求項１５記載の画像復号化装置。
【発明の詳細な説明】
【０００１】

【発明の属する技術分野】この発明は、契約したユーザに対して、その課金に応じた画像を暗号化して提供する画像符号化装置及び暗号化された画像を復号する画像復号化装置に関するものである。

【０００２】

【従来の技術】図２７は、例えば特開平6-54325号公報に示された従来の画像符号化装置及び画像復号化装置からなる画像伝送システムで、画像復号化装置の暗号解読能力に対応して異なる品質の画像を供給できるものを示す構成図である。図において、２００は画像符号化装置をあらわし、その構成要素として、２０１は入力画像を空間周波数成分に変換する直交変換手段、２０２は直交変換された画像情報を量子化し、決められた周波数領域毎に分割する量子化手段、２０３はそれぞれの周波数成分を暗号化する暗号化手段、２０４は分割された画像情報をネットワーク上に流すために一まとめにするための多重化手段を示す。　一方、３００は画像復号化装置をあらわし、その構成要素として、３０１は多重化された画像情報を再び決められた周波数成分毎に分割するための分離手段、３０２はそれぞれの周波数成分を復号化するための復号化手段、３０３は復号された各周波数成分の情報を一つにまとめそれらを逆量子化する逆量子化手段、３０４はこれらの要素を経て最後に元の画像を取り出すための逆直交変換手段をあらわしている。

【０００３】次に、動作について説明をする。はじめに、画像符号化装置２００について説明を行う。ユーザが、画像符号化装置２００に暗号化して伝送したい画像を入力すると、それらは例えば８×８ピクセルの画像領域に分割され、まず直交変換手段２０１によって例えば８×８の空間周波数成分マトリクスに変換される。出力されたマトリクスを量子化手段２０２で量子化した後、あらかじめ定められた空間周波数領域ブロックに分割されて、高周波成分のブロックから順に各暗号化手段２０３（１～n）に入力される。ここで、最も低周波成分のブロックは、暗号化が施されずに多重化手段２０４に送られる。暗号化手段２０３に入力された各空間周波数領域ブロックはあらかじめ定められた方法で暗号化が施され、多重化手段２０４に送られる。多重化手段２０４では、n+1ブロックに分割された画像情報を直列化して、ネットワーク上に出力する。これらの動作をすべての８×８ピクセルの画像領域について行うことによって、一画面の伝送が終了する。

【０００４】次に、画像復号化装置３００の動作について説明する。ネットワークから送られてきた暗号化された画像情報は、分離手段３０１によって、あらかじめ定められた空間周波数領域ブロックに分割される。各空間周波数領域ブロックは高周波成分のブロックから順に復号化手段３０２（１～n）に入力される。ここで、最も低周波成分のブロックは、復号化手段３０２を経由せずに逆量子化手段３０３に送られる。復号化手段３０２に入力された各空間周波数領域ブロックはあらかじめ定められた方法で復号化が施され、次の逆量子化手段３０３に送られる。逆量子化手段３０３では、n+1ブロックに分割された空間周波数領域ブロックを逆量子化し、さらにそれらをまとめて、例えば８×８の空間周波数成分マトリクスに変換し、逆直交変換手段３０４に出力する。逆直交変換手段３０４では、入力された空間周波数成分マトリクスから例えば８×８ピクセルの画像を取り出す。これらの動作を繰り返すことで、一画面の受信が終了する。

【０００５】画像情報を空間周波数領域で見たとき、低周波成分は画像の概形や明暗をあらわし、一方高周波成分は細かな部分をあらわしている。また、高周波成分が忠実に復元されなくても極端な画像劣化にはつながらないことが多い。従来技術ではこのような背景から、高周波成分を暗号化し、その復号機能を作動・停止することで、異なる品質の画像が再生される方法を開示している。

【０００６】

【発明が解決しようとする課題】従来の画像伝送システムで、画像復号化装置の暗号解読能力に対応して異なる品質の画像を供給できるものは、前記のように構成されており、各空間周波数領域ブロックを暗号化・復号化するための鍵は各々独立である。そのため、高い品質を要求するユーザに対しては、より多くの復号化手段を動作させる必要があるため、より多くの鍵を配送する必要があるので、画像提供者、ユーザともに多くの鍵を管理しなければならないという問題点があった。

【０００７】また、空間周波数領域分割の方法が固定的であるため、画像品質のクラス階層が固定的になってしまい、異なるクラス階層を持った画像を扱うことができないという問題点があった。

【０００８】また、画像によらず同一の鍵で暗号化、復号化が行われるため、一つの画像符号化装置に対して、対応する一つの画像復号化装置が必要であるという問題点があった。

【０００９】本発明は、前記のような問題点を解消するためになされたものであり、配送しなければならない鍵を一つにし、さらに、異なるクラス階層を持った画像の送受信を可能にし、画像に応じて、暗号化、復号化に使用する鍵を選択できる画像符号化装置及び画像復号化装置を提供することを目的とする。

【００１０】

【課題を解決するための手段】第１の発明は、画像を空間周波数成分に変換する直交変換手段と、この変換された空間周波数成分を量子化し、所定の周波数領域毎の複数のブロックに分割する量子化手段と、暗号化に使用する暗号鍵の基準となる基準鍵を用い、階層化された複数の暗号鍵を生成する鍵階層化手段と、前記量子化手段により分割されたブロックを、前記鍵階層化手段により生

成された所定の階層レベルの暗号鍵を用いて暗号化する画像暗号化手段とを備えたものである。

【００１１】第２の発明は、前記量子化手段により分割された複数のブロックをそれぞれ並列に暗号化する複数の暗号化手段と、この複数の暗号化手段により暗号化された複数のブロックを一つにまとめる多重化手段とを備えたものである。

【００１２】第３の発明は、前記階層化された複数の暗号鍵を、上位の鍵から下位の鍵を得ることができる一方向性関数により生成する鍵階層化手段を備えたものである。

【００１３】第４の発明は、前記階層化された複数の暗号鍵を、公開鍵暗号アルゴリズムにおける公開鍵を用いた暗号化により生成する鍵階層化手段を備えたものである。

【００１４】第５の発明は、前記量子化された空間周波数成分を、予め設定された周波数領域分割指定に基づいて複数のブロックに分割する量子化手段を備えたものである。

【００１５】第６の発明は、前記量子化手段により分割された各ブロックに関する情報を、前記画像暗号化手段により暗号化されたブロックに付加する暗号化情報付加手段を備えたものである。

【００１６】第７の発明は、周波数が最も高い領域のブロックを暗号化するために用いた暗号鍵の階層レベルを付加する暗号化情報付加手段を備えたものである。

【００１７】第８の発明は、乱数の発生により新しい基準鍵を生成する新規鍵生成手段と、この新規鍵生成手段により生成された新しい基準鍵を、この基準鍵を識別する鍵識別子とともに格納する鍵保存手段とを備え、前記鍵階層化手段は、前記新規鍵生成手段により生成された新しい基準鍵又は前記鍵保存手段に格納されている基準鍵のいずれかを用いて、前記階層化された複数の暗号鍵を生成するものである。

【００１８】第９の発明は、ネットワークを通じて送信されてきた所定の階層レベルの鍵要求を受信する鍵要求受信手段と、この要求された階層レベルの暗号鍵の基準となる基準鍵を、前記新規鍵生成手段により生成するか、あるいは前記鍵保存手段より取り出し、前記要求された階層レベルの暗号鍵を前記鍵階層化手段により生成する鍵取得手段と、この生成された暗号鍵を前記鍵要求の送信元に送信する鍵送信手段とを備えたものである。

【００１９】第１０の発明は、空間周波数成分に変換された画像を量子化し、暗号化して伝送された画像情報を所定の周波数領域毎の複数のブロックに分割する分離手段と、復号化に使用する復号鍵の基準となる基準鍵を用い、階層化された複数の復号鍵を生成する復号鍵階層化手段と、前記分離手段により分割されたブロックを、前記復号鍵階層化手段により生成された所定の階層レベルの復号鍵を用いて復号化する画像復号化手段とを備えたものである。

【００２０】第１１の発明は、前記分離手段により分割された複数のブロックをそれぞれ並列に復号化する複数の復号化手段と、この複数の復号化手段により復号化された複数のブロックを逆量子化し、空間周波数成分に変換する逆量子化手段と、この逆量子化手段により変換された空間周波数成分を元の画像に変換する逆直交変換手段とを備えたものである。

【００２１】第１２の発明は、前記階層化された複数の復号鍵を、上位の鍵から下位の鍵を得ることができる一方向性関数により生成する復号鍵階層化手段を備えたものである。

【００２２】第１３の発明は、前記階層化された複数の復号鍵を、公開鍵暗号アルゴリズムにおける公開鍵を用いた暗号化により生成する復号鍵階層化手段を備えたものである。

【００２３】第１４の発明は、予め設定された周波数領域分割指定に基づいて複数のブロックに分割する分離手段を備えたものである。

【００２４】第１５の発明は、外部から新しい基準鍵を入手する鍵入力手段と、この基準鍵を基準鍵識別子とともに格納する鍵保存手段とを備え、前記復号鍵階層化手段は、前記鍵入力手段により入力された新しい基準鍵又は前記鍵保存手段に格納されている前記鍵保存手段に格納されている基準鍵のいずれかを用いて、前記階層化された複数の復号鍵を生成するものである。

【００２５】第１６の発明は、基準鍵識別子に加えて鍵生成者の識別子を格納する鍵保存手段を備えたものである。

【００２６】

【発明の実施の形態】

実施の形態１．図１は、実施の形態１の画像符号化装置の構成を示す図である。図において、１は画像暗号化手段、２は画像を空間周波数成分に変換する直交変換手段、３は直交変換手段２で変換された空間周波数成分を量子化し所定の周波数領域毎に分割する量子化手段、４は量子化手段３で周波数領域毎に分割された空間周波数成分をそれぞれ暗号化する暗号化手段、５は暗号化手段４に暗号鍵を設定するとともにこの暗号鍵の基準となる基準鍵を生成する暗号化管理手段、６は暗号化管理手段５で設定された基準鍵から階層化された鍵を一方向性関数で処理し生成する鍵階層化手段、７は暗号化手段４で暗号化された分割空間周波数成分を一つにまとめる多重化手段、８は暗号化した分割空間周波数成分を送信するための画像送信手段、９はネットワークである。

【００２７】図２は、実施の形態１の画像復号化装置の構成を示す図である。図において、９は画像符号化装置で暗号化された空間周波数成分が送られてくるネットワーク、１０は画像復号化手段、１１は多重化して伝送されてきた空間周波数成分を周波数領域毎に分割するため

の分離手段、12は分離手段11で分割された空間周波数成分を復号化する復号化手段、13は復号化手段12に復号鍵を設定するとともにこの復号化に使用する鍵の基準となる基準鍵を格納する復号化管理手段、14は復号化管理手段13に格納されている基準鍵から階層化された鍵を一方向性関数で処理し生成する鍵階層化手段、15は復号化手段12で復号化された分割空間周波数成分を一つにまとめ逆量子化する逆量子化手段、16は逆量子化手段15で逆量子化された空間周波数成分を画像に変換する逆直交変換手段、17は画像を表示する画像表示手段である。

【0028】以下、本実施の形態の動作説明を行う。まず、画像符号化装置の処理について説明する。図1の画像符号化装置において画像を符号化するとき、その前処理として暗号化管理手段5は、各暗号化手段4に対して暗号化に使用する暗号鍵を設定する。このとき鍵階層化手段6を使用して各暗号化手段4に設定すべき暗号鍵を生成する。具体的には、暗号化管理手段5は、まず基準となる基準鍵を乱数を基に生成し、これを鍵階層化手段6で変換させることによって、各暗号化手段4に設定すべき暗号鍵を生成する。

【0029】ここで鍵の階層化とは、以下の2つの性質を満たすような鍵系列を、基準鍵から生成することである。(1)上位の鍵から、下位の鍵を生成することは容易であるが、(2)下位の鍵から上位の鍵を推測することは計算量的に困難である。

【0030】このように階層化された暗号鍵を、高位のものから順に暗号化手段4に設定していく。

【0031】暗号化管理手段5が、各暗号化手段4に階層化された暗号鍵を設定した後は、従来技術と同様に画像は処理されていく。すなわち、直交変換手段2で空間周波数成分に変換され、量子化手段3によって量子化された後、あらかじめ定められた空間周波数領域ブロックに分割されて、それぞれのブロックに対応した暗号化手段4によって暗号化が施され、最後に多重化手段7で直列化され、画像送信手段8、ネットワーク9を通じて画像復号化装置に画像情報は送られる。

【0032】画像符号化の前処理は、各暗号化手段4に設定する暗号鍵を、基準鍵を階層化することによって生成する方法を用いる。これにより、画像符号化装置は、ただ一つの鍵のみを管理し、暗号化時に使用する鍵は使用後破棄してしまうことが可能になる。

【0033】図3は、図1の画像符号化装置における鍵階層化手段6の鍵階層化処理の流れを示すフローチャートである。図を用いて、鍵階層化手段6の動作を説明する。鍵階層化手段6は、暗号化管理手段5によって起動される。このとき、基準鍵と必要とされる鍵の階層レベルLevelを引数として渡される。ステップS1では、一時変数Keyを基準鍵で、また一時変数nを最上位のレベルをあらわす値1で初期化する。ステップS2～ステップS4はループを形成している。ステップS2はループを抜ける条件を評価している。「n＝必要とされる鍵の階層レベルLevel」となったとき、変数Keyには、そのレベルに対応した階層化された鍵が格納されているのでKeyの内容を暗号化管理手段5に返す。もし、「n＝必要とされる鍵の階層レベルLevel」でなければ、ステップS3で鍵は一段階階層化される。その後、ステップS4で、nが1増やされる。このループをステップS2の評価が真になるまで繰り返す。

【0034】ステップS3において鍵の階層化は、鍵を一方向性関数で処理することで実現される。一方向性関数とは、逆関数を求めることが困難であるような関数を指す。このようにすることで、上位の鍵から下位の鍵を生成するのは、関数を通すだけであるため容易であるのに対し、下位の鍵から上位の鍵を生成するためには一方向性関数の逆関数を求める必要があるため困難となり、上述した階層鍵の定義を満たすような鍵系列を生成することができる。

【0035】本実施の形態例においては、上位の鍵と、下位の鍵が極力一対一の関係にあることが望ましいため、一方向性関数として、SHA, MD5などに代表されるメッセージ縮約アルゴリズムを使用している。

【0036】次に、画像復号化装置の動作について述べる。画像を復号化するとき、その前処理として復号化管理手段13は、各復号化手段12に対して、復号化に使用する復号鍵を設定する。このとき復号化管理手段13は鍵階層化手段14を使用して各復号化手段12に設定すべき復号鍵を生成する。ただし、階層化された復号鍵を生成するための基準鍵は、課金等に応じて画像送信者から渡されるものであるため、常に最上位の鍵であるとは限らず、一般に画像送信者の使用している基準鍵を何段階か階層化して得られるものである。そのため、渡された鍵の階層化レベルより上位の復号化手段には基準鍵から、より上位の鍵を生成する必要があるため、階層鍵の定義より、このような鍵は生成することが困難であり、従ってそのような復号化手段には鍵を設定することができない。

【0037】設定できる最上位の復号化手段から順に、基準鍵を階層化して得られる復号鍵を設定して、その後復号処理が開始される。復号処理は従来技術と同様である。すなわち、ネットワーク9を通じて送られてきた、暗号化された画像情報を分離手段11によってあらかじめ定められた空間周波数領域ブロックに分割し、各ブロックに対応した復号化手段12によって復号され、逆量子化手段15で逆量子化された後、空間周波数領域マトリクスに変換され、逆直交変換手段16で通常の画像に戻された後、最後に画像表示手段17によって表示される。ただし復号鍵を設定されていない復号化手段は、いかなる入力に対しても0を出力する。これにより、従来技術で言うところの復号機能の停止が実現される。

【００３８】図４は、図２の画像復号化装置における鍵階層化手段１４の鍵階層化処理の流れを示すフローチャートである。図を用いて鍵階層化手段１４の動作について説明する。鍵階層化手段１４は、復号化管理手段１３によって起動される。このとき、復号化管理手段１３から基準鍵、基準鍵が鍵系列のどの階層レベルに位置するかを示す基準レベル及び必要とされる鍵の階層レベルＬｅｖｅｌが引数として渡される。基準鍵、基準レベルはともに、あらかじめ画像送信者から画像受信者にオフラインで渡されたものであり、それらは復号化管理手段１３に格納されている。ステップＳ５では、一時変数Ｋｅｙを基準鍵で、一時変数ｎを基準レベルで初期化する。もし、「基準レベルｎ＞必要とされる鍵の階層レベルＬｅｖｅｌ」、すなわち基準レベルよりも上位レベルの鍵が要求されたならばステップＳ６の評価が真となり、その結果エラーが復号化管理手段１３に返される。ステップＳ７～ステップＳ９はループを形成している。ステップＳ７は、ループを抜ける条件を評価している。「基準レベルｎ＝必要とされる鍵の階層レベルＬｅｖｅｌ」となったとき、変数Ｋｅｙにはそのレベルに対応した階層化された鍵が格納されているので、Ｋｅｙの内容を復号化管理手段１３に返す。もし、「基準レベルｎ＝必要とされる鍵の階層レベルＬｅｖｅｌ」でなければ、ステップＳ８によって鍵は一段階階層化される。その後ステップＳ９で、ｎが１増やされる。このループをＳ７の評価が真になるまで繰り返す。

【００３９】以上のように本実施の形態では、基準となる基準鍵を階層化することによって生成する復号鍵を各復号化手段１２に設定し復号化を行うため、画像復号化装置はただ一つの鍵のみを管理し、復号化時に使用する鍵は使用後破棄してしまうことが可能になる。

【００４０】実施の形態２．図５は、実施の形態２の画像符号化置の構成を示す図である。また、図６は実施の形態２の画像復号化装置の構成及び処理の流れを示す図である。図５、図６のそれぞれに記載の画像符号化装置及び画像復号化装置とも、空間周波数成分に分割した画像情報をバッファに格納する構成である。これにより、実施の形態１において複数必要だった、画像符号化装置中の暗号化手段及び画像復号化装置中の復号化手段をそれぞれ一つで済むようにし、さらに画像符号化装置中の多重化手段及び画像復号化装置中の分離手段を省略可能にしたものである。

【００４１】図７は、画像符号化装置中の画像情報が変換されていく様子を示す図である。図５及び図７を参照しながら、本実施の形態における画像符号化装置の処理の流れについて説明する。図７において、元画像は、実施の形態１と同様に、例えば８×８ピクセル単位に分解され（ａ）、各々は直交変換及び量子化が施されて、例えば８×８の空間周波数領域マトリクスに変換される（ｂ）。その後、このマトリクスは、低周波成分から（ｃ）で示されるようにジグザグに走査されて、図５のバッファ３１に格納される。次いで、暗号化管理手段２８は、図５においてステップＳ１０、ステップＳ１１で鍵階層化手段２９を用いて暗号化するための暗号鍵を生成し、ステップＳ１２で暗号化手段３２に暗号化を行うよう要求する。この時渡されるパラメータは、鍵情報Ｋｅｙと暗号化するブロック数である。暗号化手段３２は要求を受け取ると、バッファ３１から指定されたブロック数だけデータを取り出し、指定された鍵によって暗号化し、それを暗号化された画像情報を格納するためのバッファ３３に格納する。この動作を繰り返して、バッファ３１中のデータをすべてバッファ３３に格納した段階で、元画像領域における、８×８ピクセルの暗号化が終了したことになる。これらを元画像領域全体にわたって繰り返すことで元画像を暗号化したデータが、バッファ３３に格納される。ただし、各空間周波数領域マトリクスの最も低周波部分に属するブロックは暗号化されることなくバッファ３３に出力されるものとする。最後にバッファ３３の内容を、ネットワークに送る。従って、本実施の形態におけるデータのフォーマットは、図７（ｄ）のようになる。

【００４２】図６の画像復号化装置は、実施の形態１で示した分離手段１１を取り除いた代わりに、復号化管理手段３４が復号すべきブロック数を復号化手段３７に指定することで同様な効果を得ている。処理の流れは、本実施の形態の画像符号化装置中のそれとほぼ同様である。ただし、実施の形態１の説明で述べたように、復号化のための鍵を設定できない場合、復号化手段３７は入力されたブロックに関わらず０を出力する。

【００４３】以上のように、画像情報を一度バッファに蓄えて、順番に暗号化･復号化していく方法をとることで、暗号化管理手段・復号化管理手段の設定を変えるだけで自由に画像の品質の階層を設定できるという効果が生じる。

【００４４】実施の形態３．図８及び図９は、それぞれ実施の形態３の画像符号化装置及び画像復号化装置の構成を示す図である。図８は、実施の形態２の画像符号化装置に暗号化情報付加手段４５を追加した画像符号化装置をあらわしている。また、図９は実施の形態２の画像復号化装置に暗号化情報抽出手段５２を追加した画像復号化装置をあらわしている。これにより、ネットワーク９を流れる画像情報に、暗号化する際の空間周波数領域ブロックの分割方法を記述したヘッダを付加することが可能となり、その結果、画像送信者は自由に、画像毎に異なる品質階層を設定することが可能となる。　図１０は、画像情報に付加されるヘッダの一例をあらわしたものであり、このヘッダには、画像を所定の領域に分割した時の領域分割数Ｎと、暗号化されていない周波数領域ブロック数ＢＮと、鍵の階層レベルＬｅｖｅｌＮ－１の階層鍵で暗号化された周波数領域ブロック数ＢＮ-1と、

鍵の階層レベルＬｅｖｅｌｉの階層鍵で暗号化された周波数領域ブロック数Ｂiと、鍵の階層レベルＬｅｖｅｌ１の階層鍵で暗号化された周波数領域ブロック数Ｂ1などの空間周波数領域ブロックの分割方法及び暗号化された画像情報が記述されている。

【００４５】実施の形態４．図１１は、実施の形態４の画像符号化装置において画像情報に付加されるヘッダの別の例を示す図である。実施の形態３の暗号化情報付加手段４５において、最高位の空間周波数領域ブロックを暗号化している鍵の階層化のレベルである最高品質ＬｅｖｅｌＬminもヘッダの内容に含めることで、あるレベル以上の鍵を持っているユーザは、画像を完全に復号できるような画像の配信を可能としている。

【００４６】実施の形態５．図８に示した画像符号化装置の鍵階層化手段４３において、一方向性関数処理に公開鍵暗号系アルゴリズムを用い、画像送信者の公開鍵により暗号化することで、それまで最上位の鍵からさらに上位の鍵を生成することが可能になる。

【００４７】図１２は、実施の形態５の画像符号化装置の階層鍵生成手段の処理の流れを示すフローチャートである。図１２のフローチャートを用いて、実施の形態５の画像符号化装置の鍵階層化手段の処理の流れを説明する。鍵階層化手段４３は、暗号化管理手段４４によって起動される。このとき、基準鍵と必要とされる鍵の階層レベルＬｅｖｅｌを引数として渡される。しかし、本実施の形態では、必要とされる鍵の階層レベルは、基準鍵よりも高いレベル、すなわち０以下の値をとることも可能である。

【００４８】ステップＳ１６で、一時変数Ｋｅｙを基準鍵で、一時変数ｎを最上位のレベルをあらわす値１で初期化する。ステップＳ１７で、「ｎ＝必要とされる鍵の階層レベルＬｅｖｅｌ」になったら、その時Ｋｅｙに入っている値がそのレベルに対応する鍵データであるのでその値を返して終了する。もし「ｎ＝必要とされる鍵の階層レベルＬｅｖｅｌ」でなかったならば、ステップＳ１８に移る。ステップＳ１８では、望まれる鍵の階層レベルＬｅｖｅｌが最上位のレベルの１よりも高いレベルかどうかを判別している。もしも、「必要とされる鍵の階層レベルＬｅｖｅｌ＜１」でなかったら（Ｌｅｖｅｌ≧１）、ステップＳ１９で、画像送信者の公開鍵によって暗号化されることで一段階階層化され、ステップＳ２０でｎを一つ増やし、ステップＳ１７で再評価される。

【００４９】一方、「必要とされる鍵の階層レベルＬｅｖｅｌ＜１」であったら、ステップＳ２１で、画像送信者の秘密鍵によって暗号化されることで逆方向に一段階階層化される。なぜならば、このようにして生成された鍵を、本実施の形態における一方向性関数である画像送信者の公開鍵によって暗号化することで、秘密鍵による暗号化が復号されて元の鍵を得ることができるからである。次にステップＳ２２においてｎを一つ減じてステップＳ１７で再評価される。

【００５０】実施の形態６．図１３、図１４は、それぞれ実施の形態６の画像符号化装置及び画像復号化装置の構成を示す図である。図１３は、図８に示す画像符号化装置３９の構成に、鍵管理手段６１、新規鍵生成手段６２、鍵保存手段６３、鍵出力手段６４を追加した画像符号化装置である。また、図１４は図９に示す画像復号化装置に、鍵管理手段７３、鍵保存手段７４、鍵入力手段７５を追加した画像復号化装置である。図１５は画像符号化装置において、既存の鍵を再利用する場合の処理の流れを、また図１６は新規に鍵を生成する場合の処理の流れを示す図である。さらに、図１７は画像符号化装置の鍵保存手段６３において鍵が格納されている様子をあらわす図である。図１８は、画像符号化装置中の鍵出力手段６４において鍵の出力形式を示す図である。また、図１９は、ネットワーク９を通じて送信される画像情報に付加されるヘッダを、図２０は画像復号化装置中において必要な鍵を鍵保存手段７４から取得する様子を示す図である。図２１は、画像復号化装置の鍵保存手段７４における鍵の保存形式をあらわす図である。

【００５１】次に、図１３の画像符号化装置で画像を暗号化するときの動作について説明する。画像を暗号化する際、暗号化管理手段５６は画像送信者の設定によって、既存の鍵を使用して暗号化するか、新規に鍵を生成して暗号化するかを決定する。既存の鍵は鍵保存手段６３に、図１７に示すように、一意に割り振られた識別子をキーとして格納されている。既存の鍵を利用して画像の暗号化を行う場合の処理の流れは、図１５のようになる。暗号化管理手段５６から鍵の要求を受け取った鍵管理手段６１は、引数として、鍵を指し示す鍵識別子を受け取る（ステップＳ２３）。鍵管理手段６１は、鍵保存手段６３に対して鍵識別子をキーとして対応する鍵を返すよう要求する（ステップＳ２４）。鍵保存手段６３は、与えられた鍵識別子をキーとして、自分の保持している鍵データを検索する（ステップＳ２５）。もし、対応する鍵が鍵保存手段６３中に存在していたならば、鍵保存手段６３は鍵識別子とともに、対応する鍵を返す（ステップＳ２６）。これらを受け取った鍵管理手段６１は、それらを暗号化管理手段５６に渡す（ステップＳ２７）。

【００５２】新規に鍵を生成して画像の暗号化を行う場合の処理は、図１６のようになる。新規の鍵を生成する要求を受けた鍵管理手段６１は（ステップＳ２８）、新規鍵生成手段６２に鍵生成要求を出す（ステップＳ２９）。新規鍵生成手段６２は、内部で乱数を発生することによって新しい鍵を生成し（ステップＳ３０）、その結果を鍵管理手段６１に返す（ステップＳ３１）。次に鍵管理手段６１は鍵保存手段６３に対して、今生成した鍵を保存するように要求する（ステップＳ３２）。　鍵

保存手段６３は、まだ使用していない識別子をその鍵に対して割り当て（ステップＳ３３）、新しい鍵を格納し（ステップＳ３４）、その識別子を鍵管理手段６１に返す（ステップＳ３５）。これを受け取った鍵管理手段６１は、鍵識別子と鍵を暗号化管理手段５６に渡す（ステップＳ３６）。

【００５３】画像を送信する際に、暗号化管理手段５６は、暗号化情報付加手段６０を通じて、図１１で示したヘッダ情報に加えて鍵識別子を付加する。そのため、送信される画像に付加されるヘッダ情報は図１９のようになる。

【００５４】鍵出力手段６４は、画像受信者に対して鍵を渡す必要があるときに、鍵を持ち運び可能な媒体に出力するための手段である。鍵を出力する必要が生じたならば、鍵出力手段６４は、鍵管理手段６１を通じて必要な鍵を入手し、それを鍵階層化手段５７によって階層化を施した後、鍵を持ち運び可能な媒体に出力する。図１８は出力される鍵情報の内容を表している。

【００５５】次に、図１４の画像復号化装置６５で画像を復号化するときの動作について説明する。ネットワーク９から、画像受信手段６７を通じて画像情報を受信した画像復号化装置６５は、暗号化情報抽出手段７２において、図１９に示したヘッダ情報より鍵識別子等の情報を入手し、これらを復号化管理手段７１に渡す。復号化管理手段７１は、図２０に示す処理にしたがって、鍵管理手段７３から鍵を入手する。復号化管理手段７１は、鍵管理手段７３に鍵識別子を引数として、既存鍵取得要求を行う（ステップＳ３７）。さらに、鍵管理手段７３は鍵保存手段７４に鍵識別子を引数として既存鍵の取得要求を行う（ステップＳ３８）。鍵保存手段７４では、鍵は図２１であらわされるような形式で格納されており、鍵識別子をキーとして鍵の検索が行われる（ステップＳ３９）。鍵識別子で区別される鍵が鍵保存手段７４中に存在したならば、対応する鍵とその鍵の施されている階層化レベルを鍵管理手段７３に返す（ステップＳ４０）。これを受け取った鍵管理手段７３は、復号化管理手段７１に、この鍵と階層化レベルを返す（ステップＳ４１）。

【００５６】なお、外部から新たに鍵を入手するためには鍵入力手段７５を使用する。鍵入力手段７５は持ち運び可能な記録媒体に、図１７であらわされるように記録された鍵を読み出して鍵保存手段７４中に格納する。

【００５７】実施の形態７．図２２は、実施の形態７の画像復号化装置の鍵保存手段における鍵保存テーブルの形式を示す図である。実施の形態７は、図１４に示す画像復号装置６５の鍵保存手段７４に鍵識別子に加えて鍵生成者の識別子を格納することで、異なる画像送信者が生成した鍵を一つの画像復号装置６５で管理することが可能になることをあらわしている。

【００５８】実施の形態８．図２３、図２４は、それぞれ実施の形態８の画像符号化装置及び画像復号化装置の構成を示す図である。図２３は、図１３に示す画像符号化装置５４の構成に、鍵取得手段８５、鍵要求受信手段８６、鍵送信手段８７、認証手段８８を加えた画像符号化装置を示す図である。図２４は、図１４に示す画像復号化装置６５の構成に、鍵要求送信手段１００、鍵受信手段１０１、認証手段１０２を加えた画像復号化装置７６を示す図である。さらに図２５は、本実施の形態における鍵要求メッセージのデータ形式を示す図であり、図２６は、本実施の形態における鍵配布メッセージのデータ形式を示す図である。本実施の形態を用いることで、鍵を画像符号化装置から画像復号化装置にオンラインで配送することが可能となる。

【００５９】図２４を参照しながら、画像復号化装置９０が画像を受信してから、必要な鍵を入手するまでの流れを説明する。復号化管理手段９６が、復号化に必要な鍵を鍵管理手段９８から入手しようとする。鍵管理手段９８は、実施の形態６と同様に鍵保存手段９９から対応する鍵を入手しようと試みる。鍵保存手段９９中に対応する鍵が格納されていなかった場合、ユーザにそのことを告げるメッセージを出力して、画像の送りもとの画像符号化装置７６から鍵を入手するかどうかを選択させる。もし鍵を入手するのならば階層レベルもユーザによって入力されなければならない。鍵を入手する場合、鍵管理手段９８は鍵要求送信手段１００を通じて、鍵を配送するよう画像符号化装置７６に要求する。送信されるメッセージは、図２５（ａ）であらわされるデータ形式を取る。このように、メッセージにディジタル署名を施すことによって、送信されるメッセージの改ざんや、第三者のなりすましを防止することができる。送信した鍵要求メッセージに呼応する形で、図２５（ａ）の形式であらわされる鍵要求メッセージが画像復号化装置９０に届けられ、これが鍵受信手段１０１によって暗号化を解かれた後、鍵管理手段９８に送られる。鍵管理手段９８は認証手段１０２を用いて、メッセージが本当に望まれた画像符号化装置７６から送られてきたものかどうかを認証する。認証が正しければ、鍵管理手段９８は鍵保存手段９９中に入手した鍵を保存し、復号化管理手段９６に入手した鍵とその階層化レベルを返す。

【００６０】次に、画像符号化装置７６において、鍵要求メッセージを受信してからの処理の流れを説明する。鍵要求受信手段８６によって受け取られた鍵要求メッセージは、鍵取得手段８５に届けられる。鍵取得手段８５は、認証手段８８を用いて鍵要求メッセージに付けられたディジタル署名を確認し、メッセージ送信者を確認する。メッセージ送信者を確認した後、鍵取得手段８５はメッセージ中に記述されている鍵識別子をもとに、鍵管理手段８２に対応する鍵を要求する。次に、入手した鍵を、鍵要求メッセージ中に記述されている階層レベルまで、鍵階層化手段７９を用いて階層化し、それによって

得た鍵を、鍵送信手段８７に送る。鍵送信手段８７は、鍵にディジタル署名を施し、さらに鍵要求メッセージ送信者の公開鍵によってメッセージ全体を暗号化し、送信する。なお、画像符号化装置７６から送信される鍵送信メッセージは図２６（ａ）であらわされるデータ形式である。

【００６１】以上のように、鍵を暗号化して送信する機能及び各メッセージにディジタル署名を施す機能を追加したことによりオンラインによる鍵の配送が可能になる。

【００６２】また、鍵要求メッセージにおいて、図２５（ｂ）のように公開鍵証明証の代わりに、それを一意に指し示すIssuerとシリアル番号を入れることにより、送信するメッセージの大きさを小さくすることができる。

【００６３】また、鍵要求メッセージにおいて、図２５（ｃ）のように、全体を相手の公開鍵で暗号化することにより、第三者に、どのような鍵を要求しているかの情報が漏洩することを防ぐことができる。

【００６４】さらに、鍵送信メッセージにおいて、図２６（ｂ）のように、鍵識別子と階層化レベルも含めてディジタル署名を施すことによって、鍵の送信者が偽りの鍵を送信することを防ぐことができる。

【００６５】

【発明の効果】本発明は、以上説明したように構成されているので、以下に示すような効果を奏する。

【００６６】第１の発明では、暗号化に使用する暗号鍵を暗号鍵の基準となる基準鍵を階層化することにより生成し、所定の階層レベルの暗号化鍵を用いて暗号化するので、画像符号化装置はただ一つの鍵のみのでの管理が可能になる。

【００６７】第２の発明では、量子化手段により分割された複数の周波数ブロックをそれぞれ並列に複数の暗号化手段により暗号化するため、各周波数ブロックが同時に暗号化でき、短時間での暗号化処理が可能になる。

【００６８】第３の発明では、鍵の階層化を一方向性関数で処理することにより、上位の鍵から下位の鍵を容易に得ることができ、ただ一つの鍵のみでの管理が可能になる。

【００６９】第４の発明では、公開鍵暗号アルゴリズムにおける公開鍵を用いた暗号化により、それまでの最上位の鍵からさらに上位の鍵を生成することが可能になる。

【００７０】第５の発明では、量子化された空間周波数成分をあらかじめ設定された周波数領域分割指定に基づいて複数のブロックに分割するため、様々な画像品質の階層設定化が可能となり、異なる階層の画像の配信が可能になる。

【００７１】第６の発明では、暗号化した周波数ブロックにこのブロックに関する情報を付加することにより、画像送信者は自由に画像毎に異なる品質階層を設定することができる。

【００７２】第７の発明では、最高位の周波数領域ブロックを暗号化している鍵の階層化のレベルを、暗号化した周波数ブロックに付加することにより、あるレベル以上の鍵を持っているユーザは画像を完全に復号できるような画像の配信が可能となる。

【００７３】第８の発明では、新規鍵生成手段により生成された新しい基準鍵又は鍵保存手段に格納されている基準鍵のいずれかにより暗号鍵を生成することができる。

【００７４】第９の発明では、ネットワークを通じて送信されてきた鍵要求に対する暗号鍵をネットワークを通じてオンラインで配送ができる。

【００７５】第１０の発明では、復号化に使用する復号鍵を復号鍵の基準となる基準鍵を階層化することにより生成し、所定の階層レベルの復号鍵を用いて復号化するので、画像復号化装置はただ一つの鍵のみのでの管理が可能になる。

【００７６】第１１の発明では、分離手段により分割された複数の周波数ブロックをそれぞれ並列に複数の復号化手段により復号化するため、各周波数ブロックを同時に復号化でき、短時間での復号化処理が可能になる。

【００７７】第１２の発明では、鍵の階層化を一方向性関数で処理することにより、上位の鍵から下位の鍵を容易に得ることができ、ただ一つの鍵のみでの管理が可能になる。

【００７８】第１３の発明では、公開鍵暗号アルゴリズムにおける公開鍵を用いた暗号化により、それまでの最上位の鍵からさらに上位の鍵を生成することが可能になる。

【００７９】第１４の発明では、あらかじめ設定された周波数領域分割指定に基づいて複数のブロックに分割して復号化するため、短時間で復号化処理ができる。

【００８０】第１５の発明では、外部から入手した新しい基準鍵又は鍵保存手段に格納されている基準鍵のいずれかにより復号鍵を生成することができる。

【００８１】第１６の発明では、基準鍵識別子に鍵生成者の識別子を付加することで、異なる画像送信者が生成した鍵を一つの画像復号装置中で管理することが可能になる。

【図面の簡単な説明】

【図１】　実施の形態１の画像符号化装置の構成図である。

【図２】　実施の形態１の画像復号化装置の構成図である。

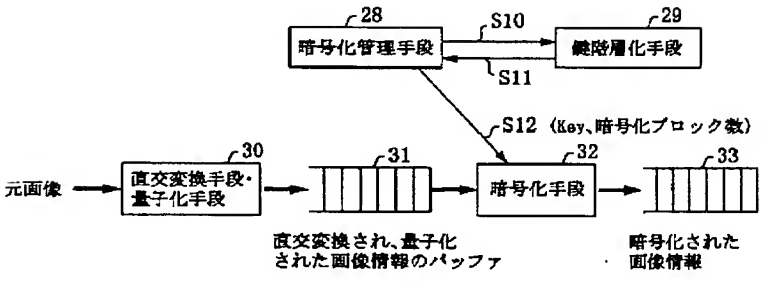
【図３】　実施の形態１の画像符号化装置における鍵階層化手段の処理の流れを示すフローチャートである。

【図４】　実施の形態１の画像復号化装置における鍵階層化手段の処理の流れを示すフローチャートである。

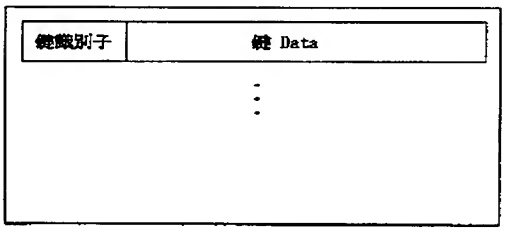
【図５】　実施の形態２の画像符号化装置の構成及び処

理の流れを示す図である。
【図６】　実施の形態２の画像復号化装置の構成及び処理の流れを示す図である。
【図７】　実施の形態２の画像符号化装置中における画像情報の変換されていく様子をあらわした図である。
【図８】　実施の形態３の画像符号化装置の構成図である。
【図９】　実施の形態３の画像復号化装置の構成図である。
【図１０】　実施の形態３の暗号化された画像情報のヘッダ部分を示す図である。
【図１１】　画像情報のヘッダ部分の別の例を示す図である。
【図１２】　実施の形態５の画像符号化装置における鍵階層化手段の処理の流れを示すフローチャートである。
【図１３】　実施の形態６の画像符号化装置の構成図である。
【図１４】　実施の形態６の画像復号化装置の構成図である。
【図１５】　実施の形態６の画像符号化装置において、既存の鍵を再使用する場合の処理の流れを示す図である。
【図１６】　実施の形態６の画像符号化装置において、新規に鍵を生成する場合の処理の流れを示す図である。
【図１７】　実施の形態６の画像符号化装置の鍵保存手段における鍵保存テーブルの形式を示す図である。
【図１８】　実施の形態６の画像符号化装置の鍵出力手段における鍵の出力形式を示す図である。
【図１９】　実施の形態６の画像符号化装置の暗号化された画像情報に付加されたヘッダ部分を示す図である。
【図２０】　実施の形態６の画像復号化装置において、既存の鍵を検索する場合の形式を示す図である。
【図２１】　実施の形態６の画像復号化装置の鍵保存手段における鍵保存テーブルの形式を示す図である。
【図２２】　実施の形態７の画像復号化装置の鍵保存手段における鍵保存テーブルの形式を示す図である。
【図２３】　実施の形態８の画像符号化装置の構成図である。
【図２４】　実施の形態８の画像復号化装置の構成図である。
【図２５】　実施の形態８の鍵要求メッセージのデータ形式である。
【図２６】　実施の形態８の鍵送信メッセージのデータ形式である。
【図２７】　従来の画像伝送システムの構成図である。
【符号の説明】
１　画像暗号化手段、２　直交変換手段、３　量子化手段、４　暗号化手段、５　暗号化管理手段、６　鍵階層化手段、７　多重化手段、８　画像送信手段、９　ネットワーク、１０　画像復号化手段、１１　分離手段、１２　復号化手段、１３　復号化管理手段、１４　鍵階層化手段、１５　逆量子化手段、１６　逆直交変換手段、１７　画像表示手段。

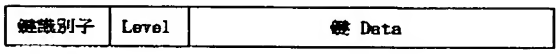
【図５】



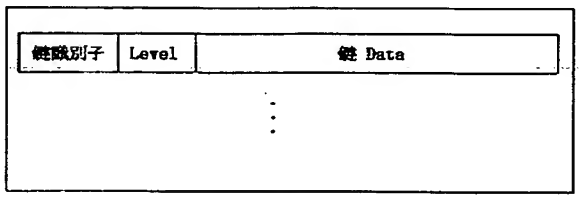
【図１７】



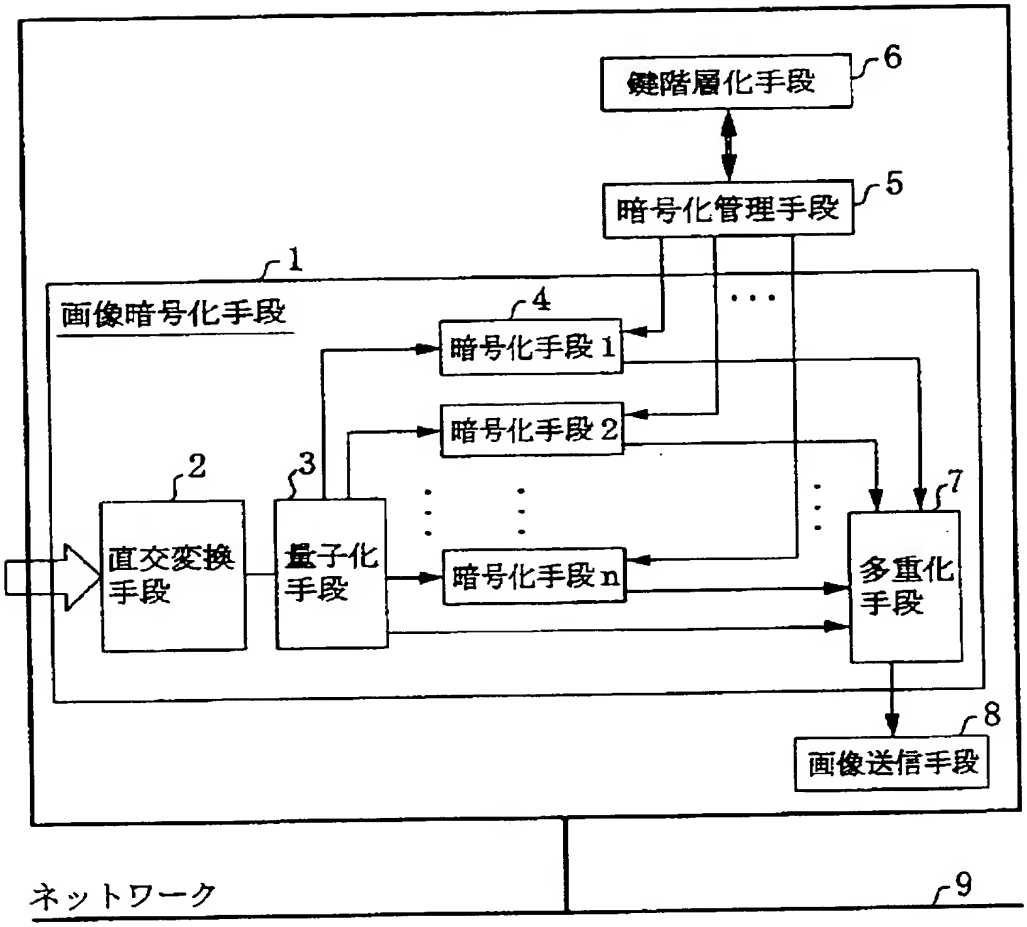
【図１８】



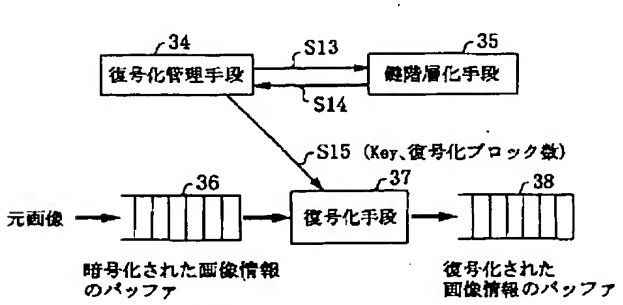
【図２１】



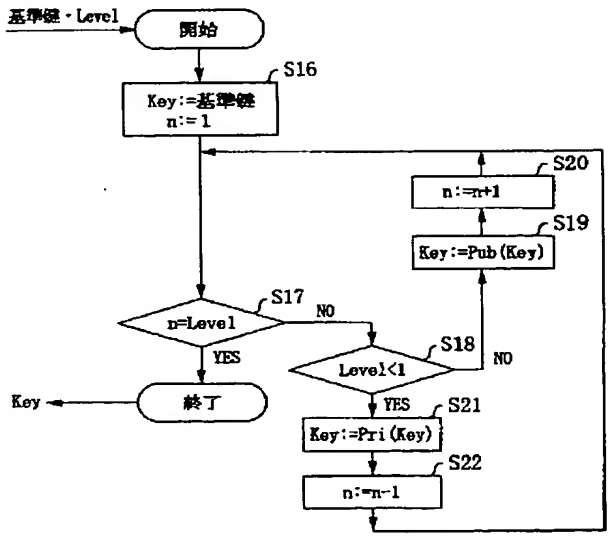
【図１】



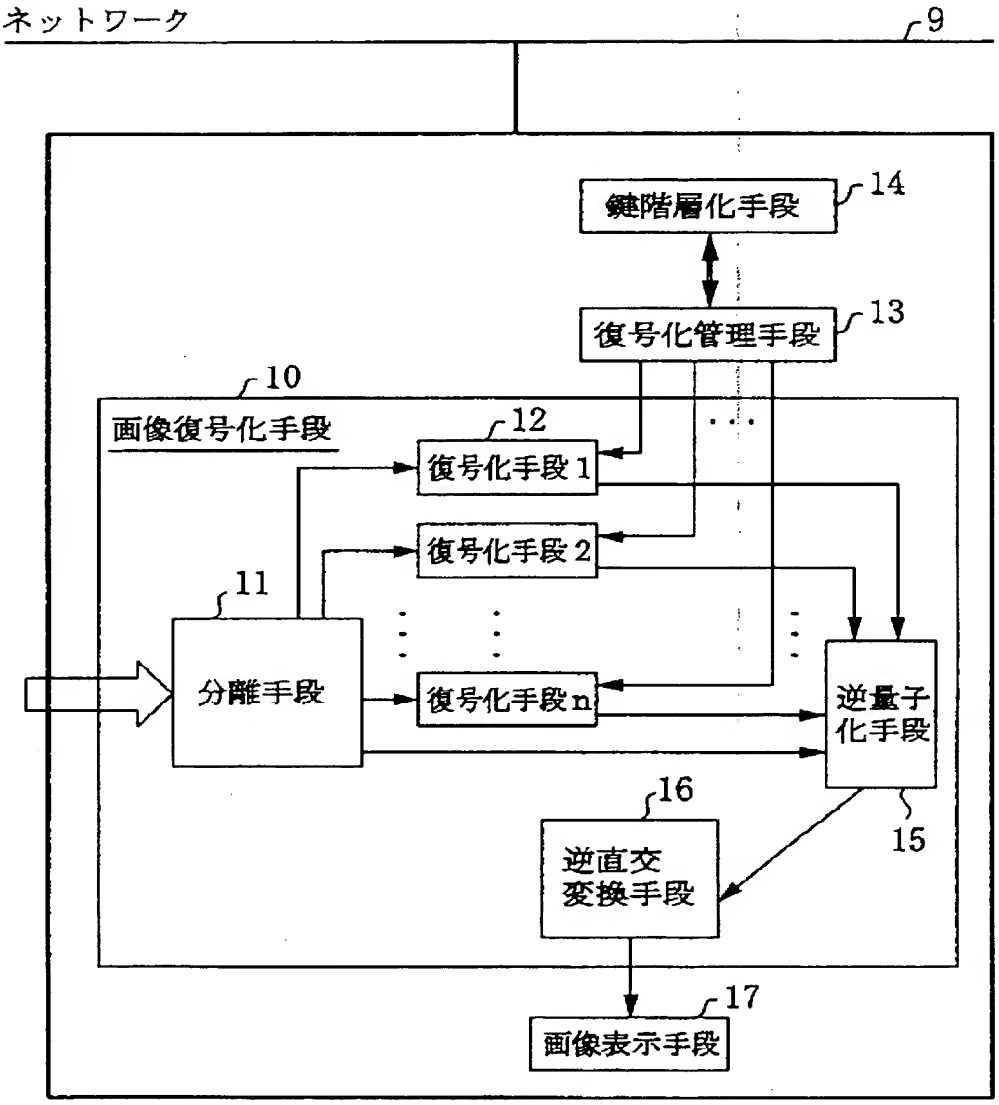
【図６】



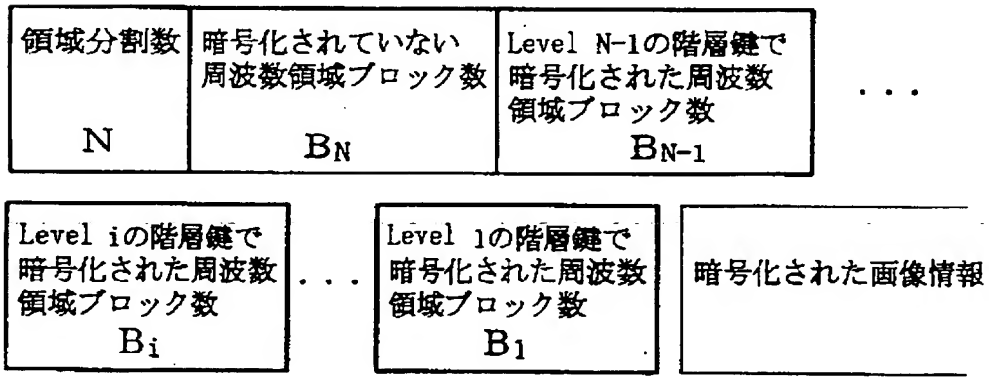
【図１２】



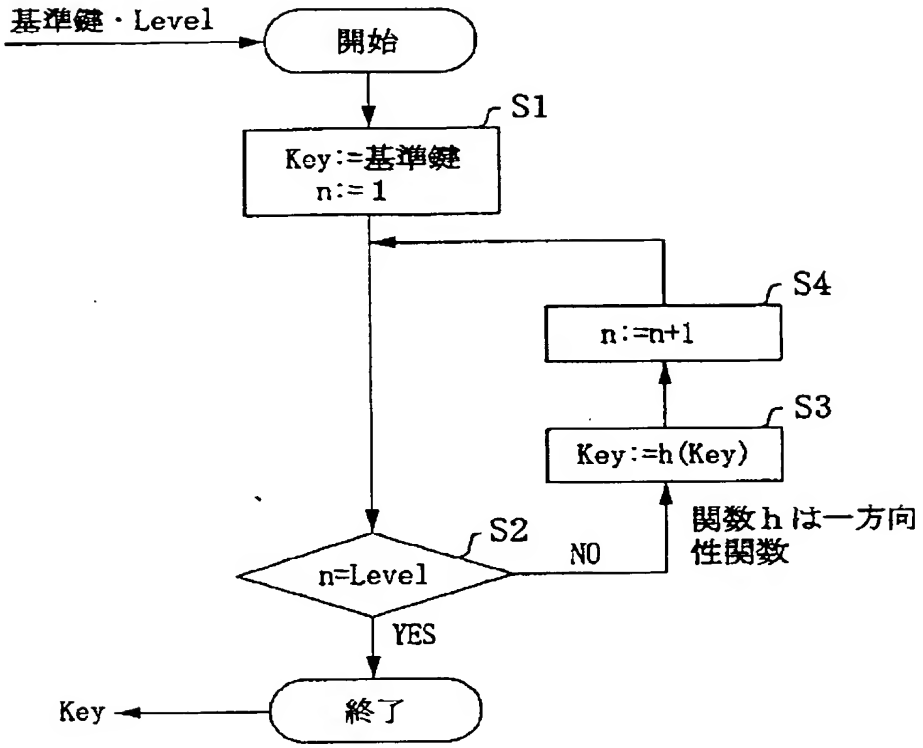
【図2】



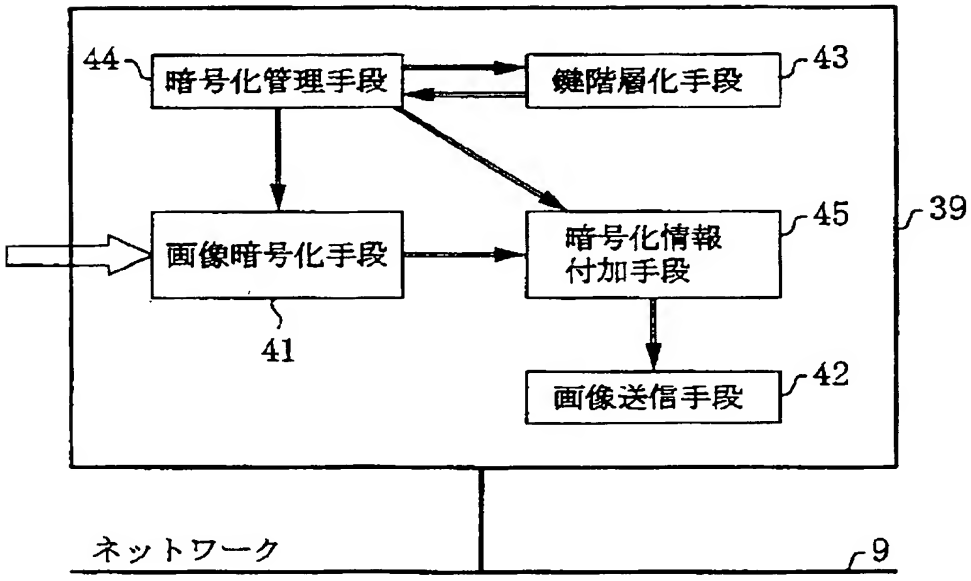
【図10】



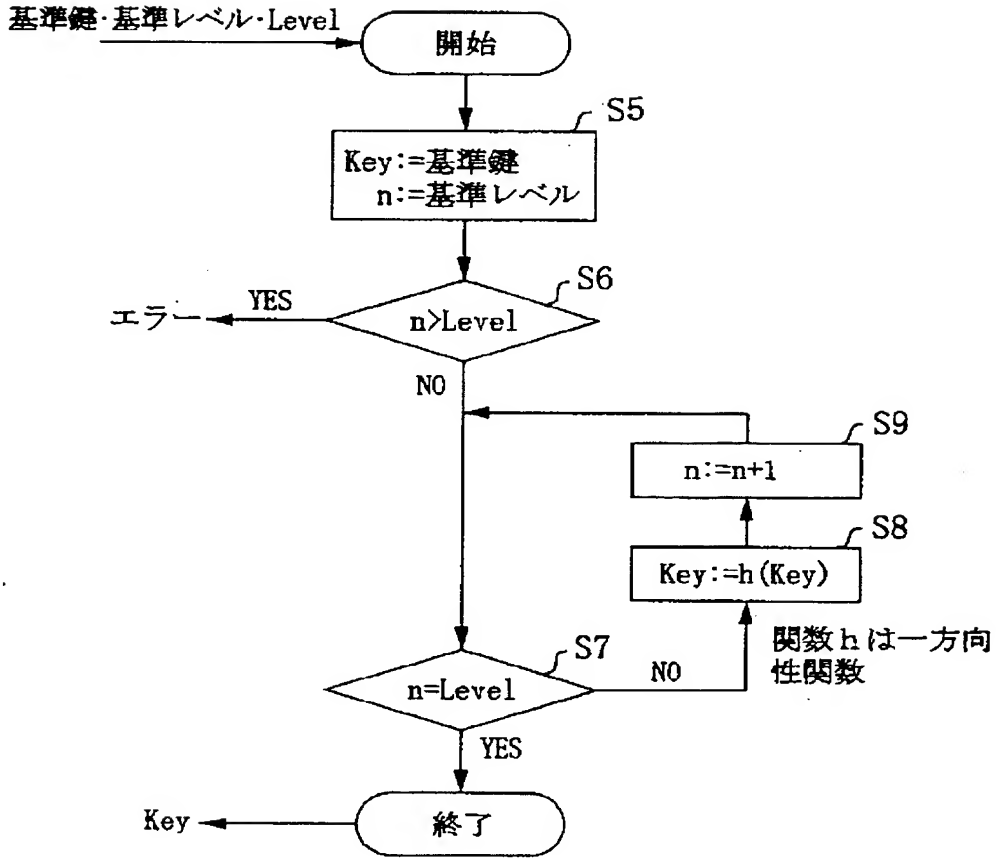
【図３】



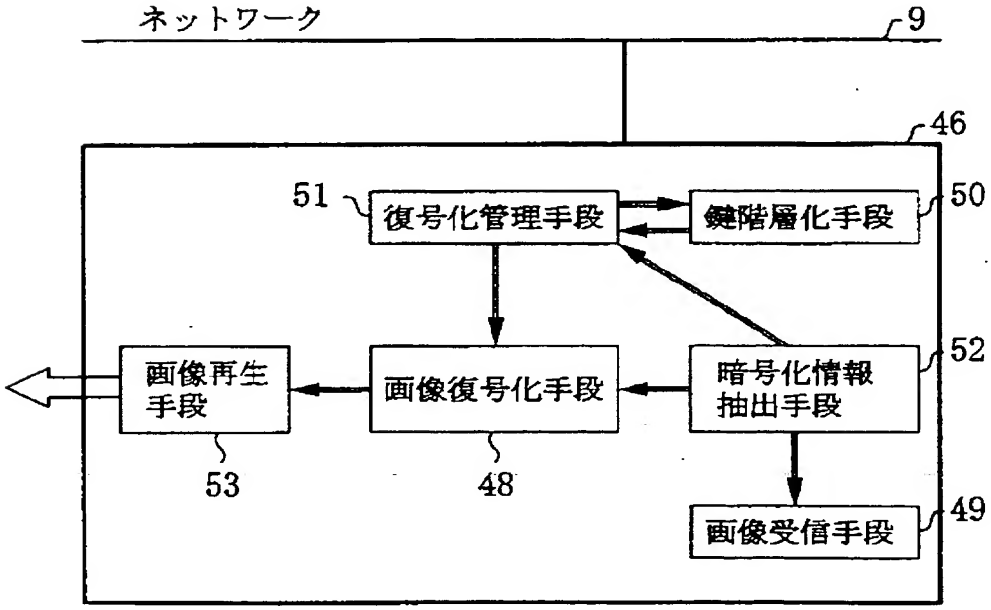
【図８】



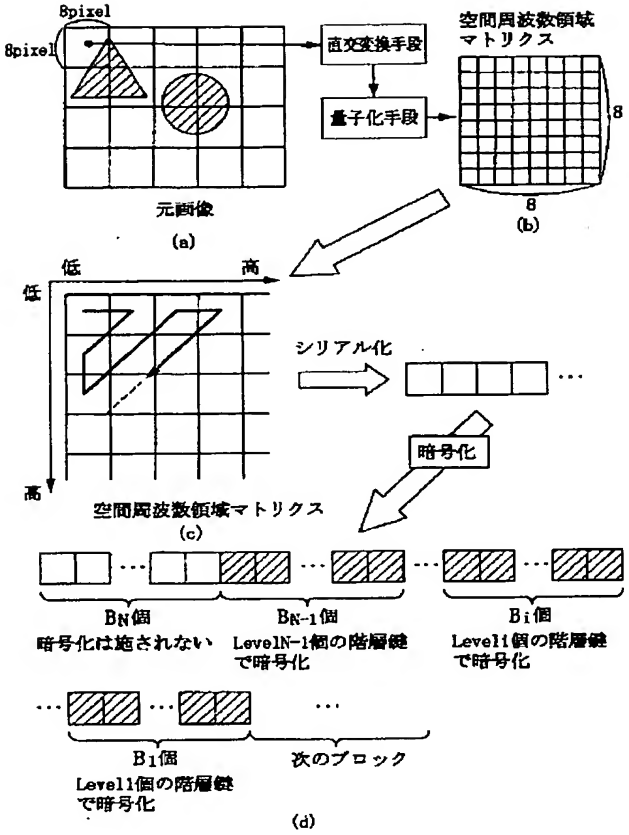
【図４】



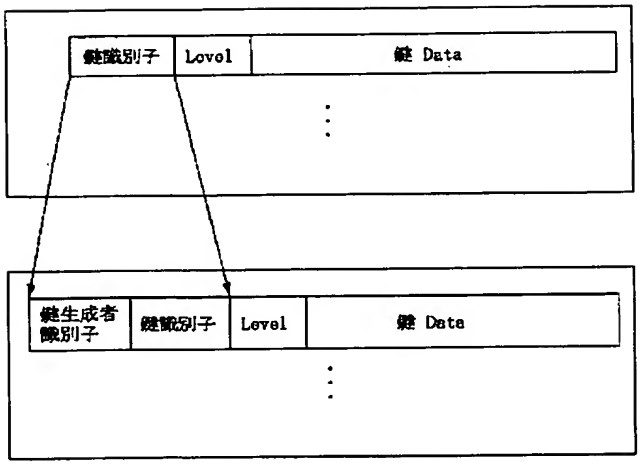
【図９】



【図7】



【図22】



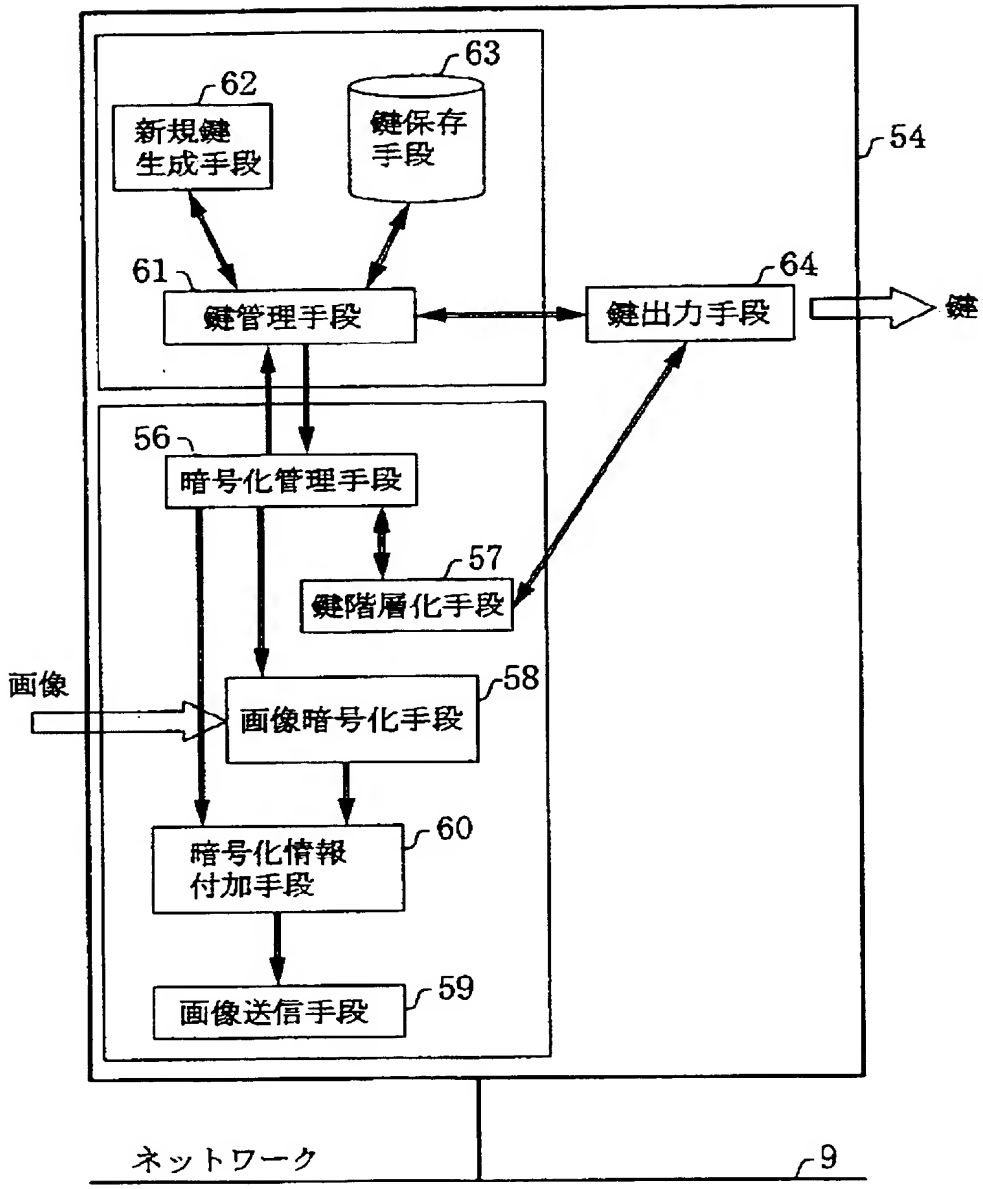
【図11】

領域分割数 N	最高品質 Level L_{min}	暗号化されていない 周波数領域ブロック数 $B_{N+Lmin-1}$	Level N-1+Lmin-1の階層鍵で暗号化された 周波数領域ブロック数 $B_{N-1-Lmin-1}$

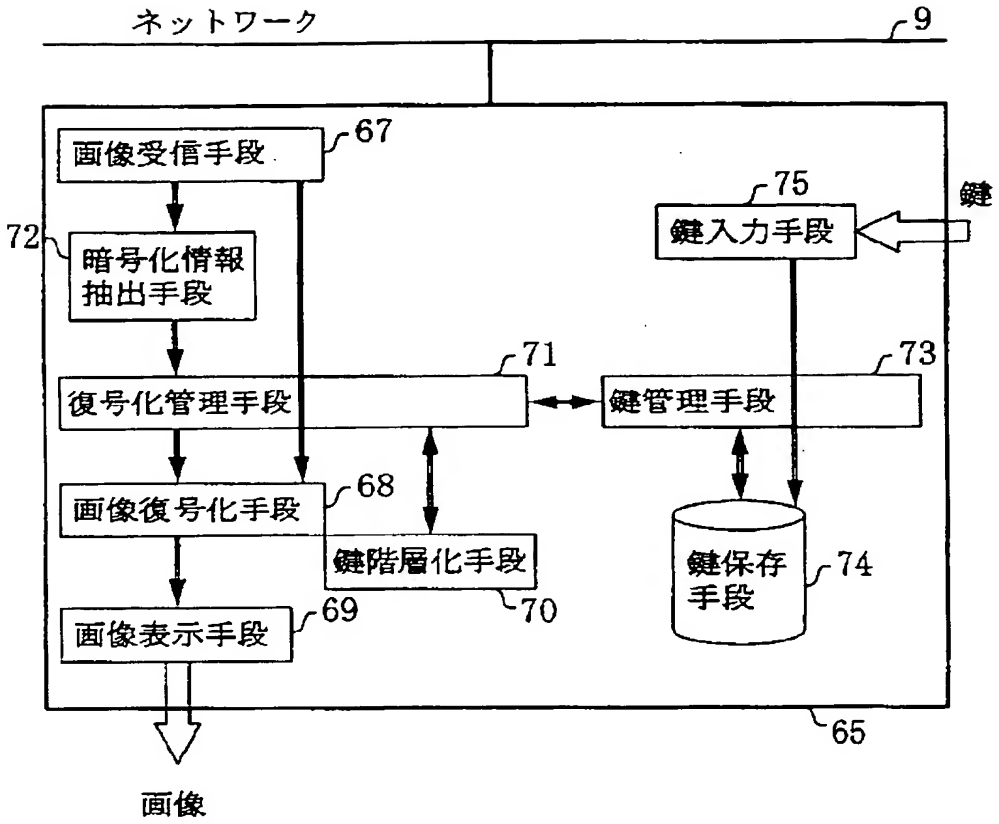
. . .

Level iの階層鍵で暗号化された周波数領域ブロック数 B_i	. . .	Level Lminの階層鍵で暗号化された周波数領域ブロック数 B_{Lmin}	暗号化された画像情報

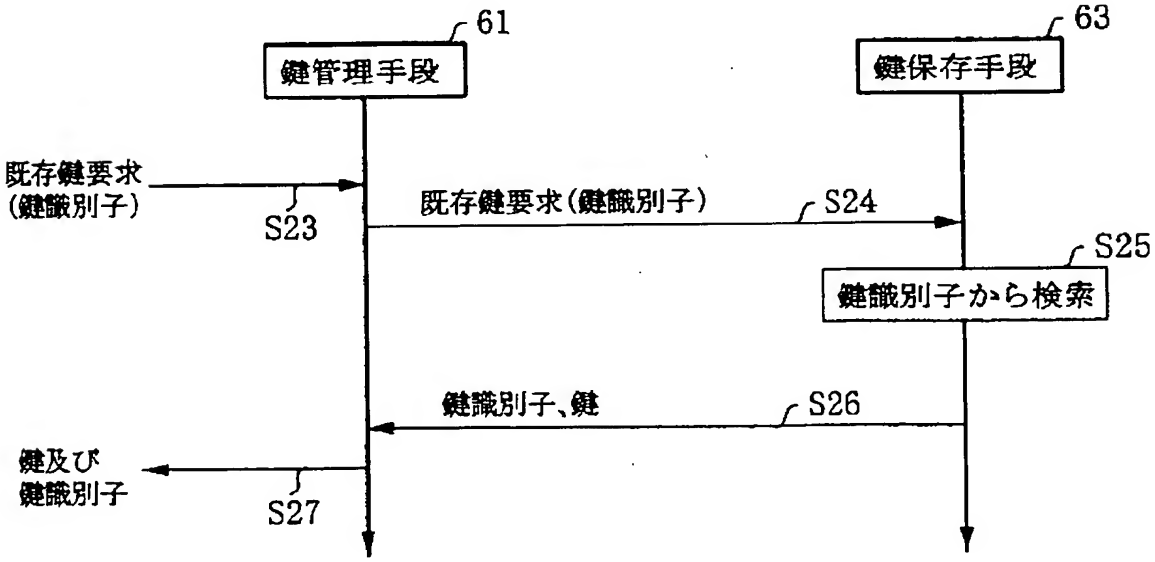
【図13】



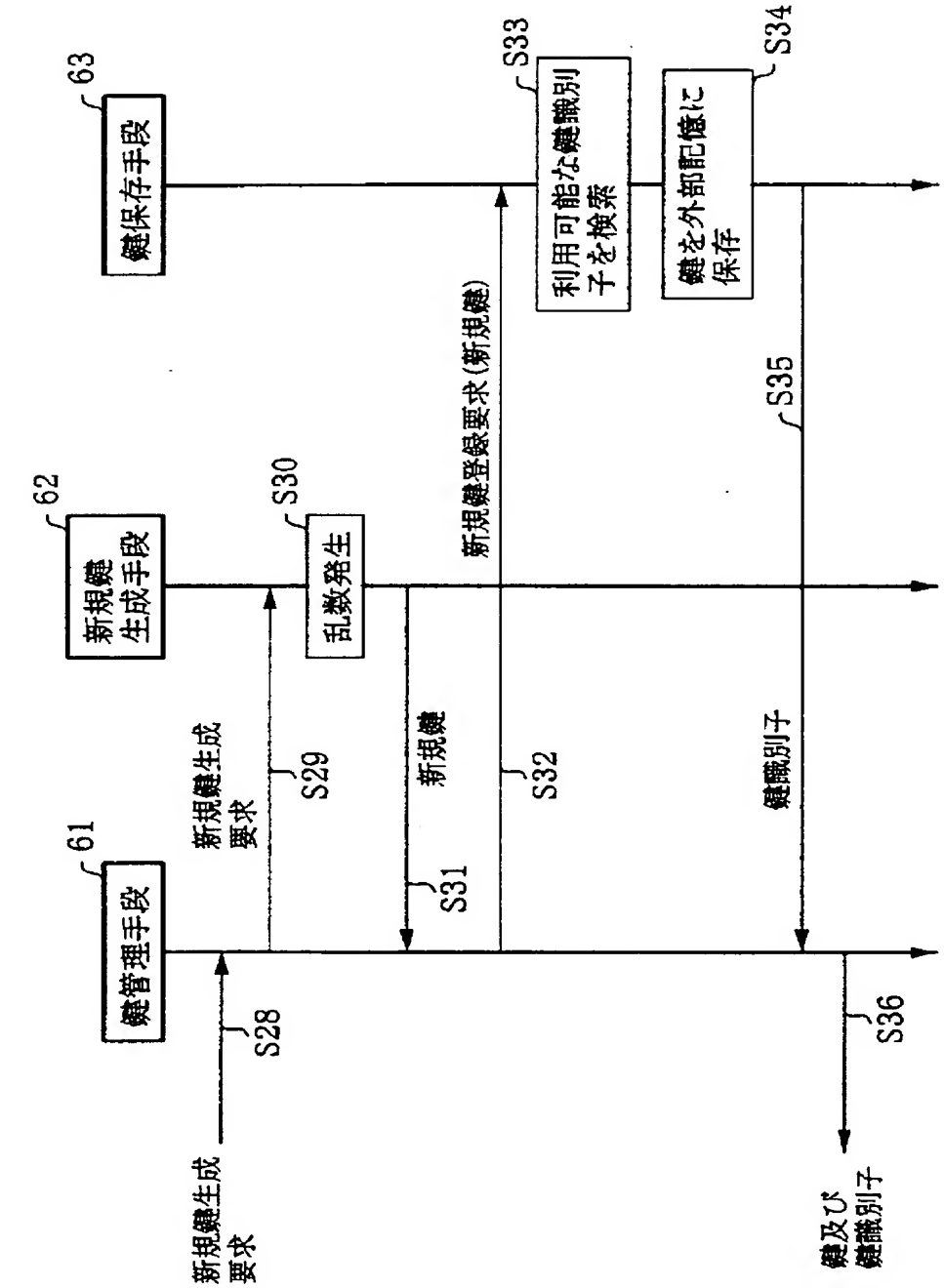
【図14】



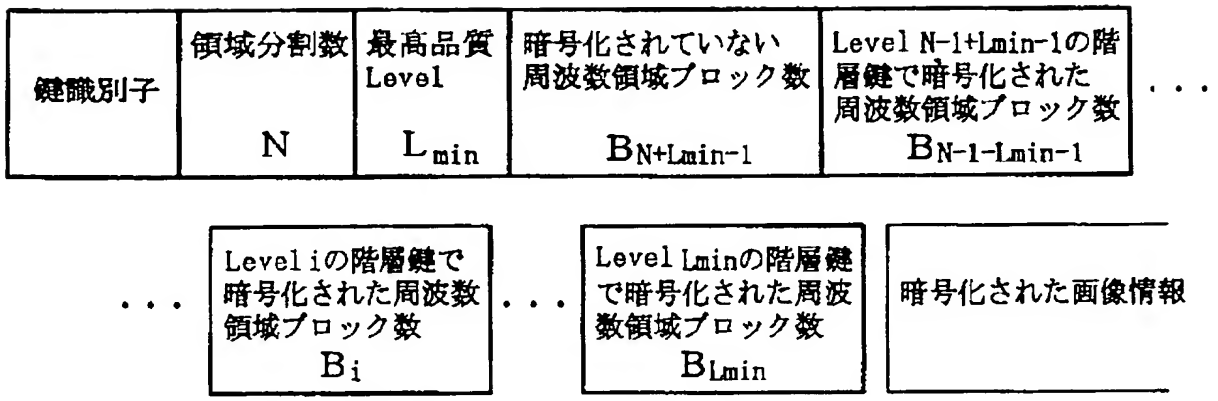
【図15】



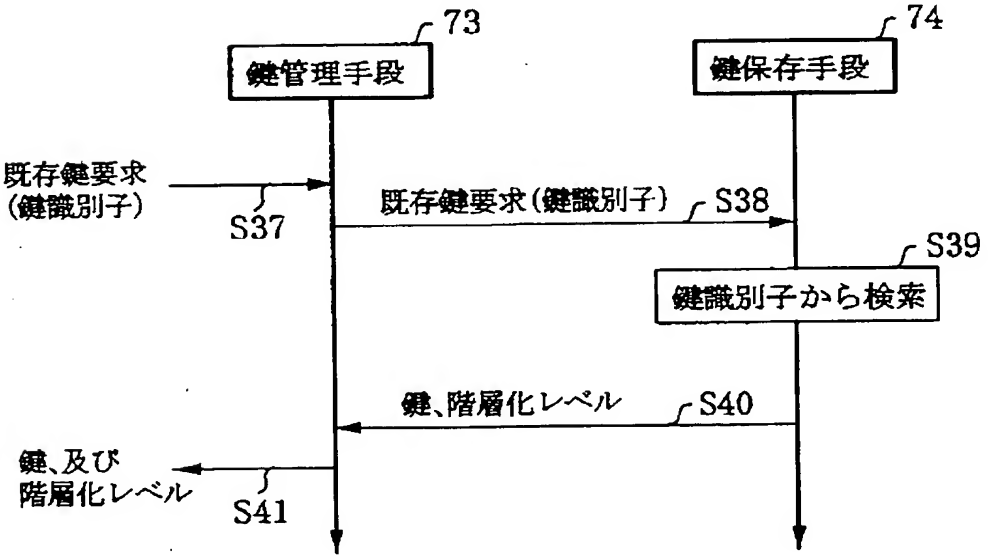
【図16】



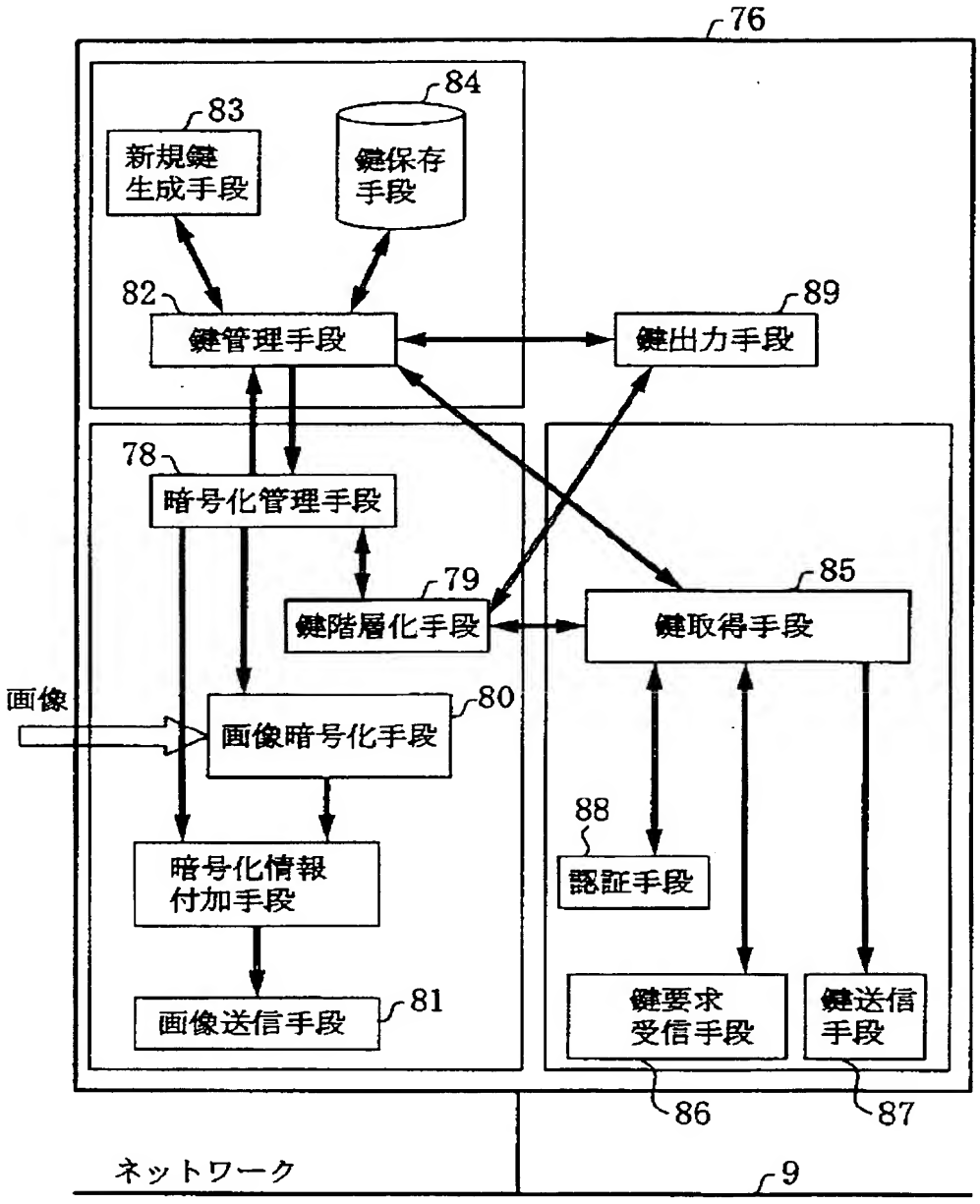
【図19】



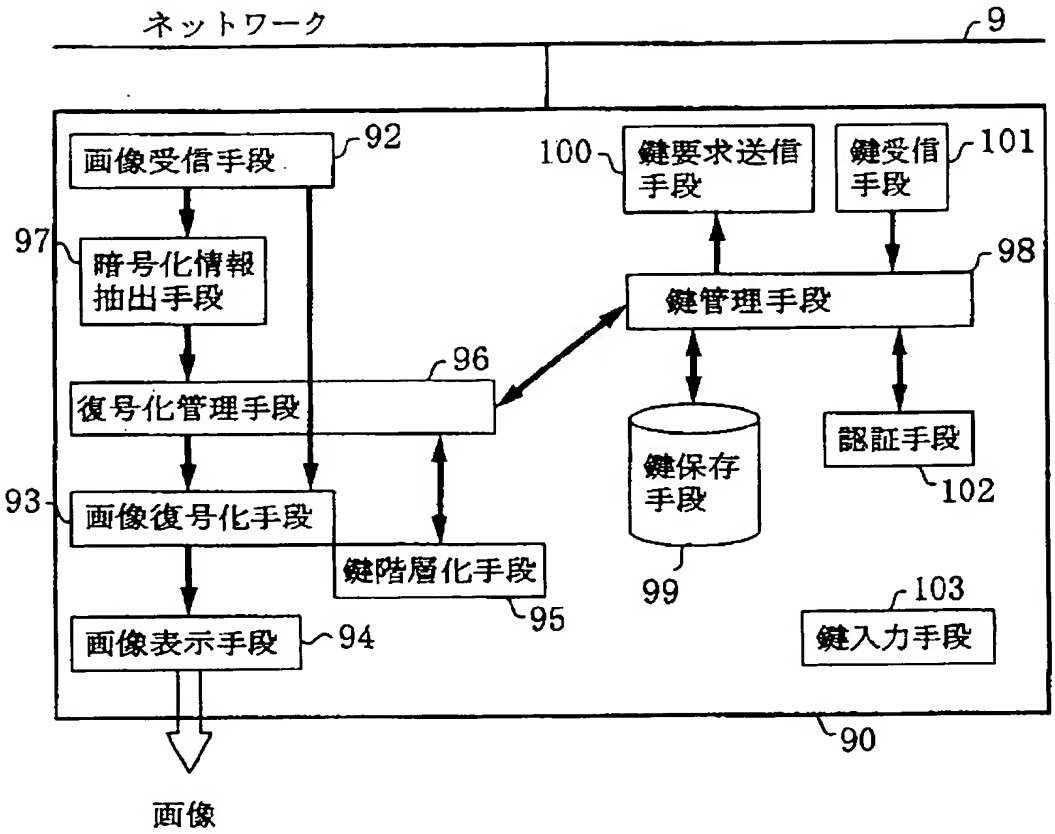
【図20】



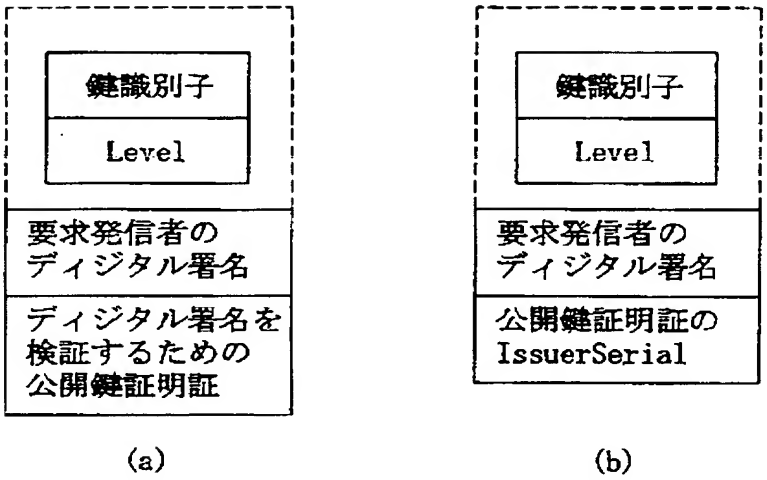
【図２３】



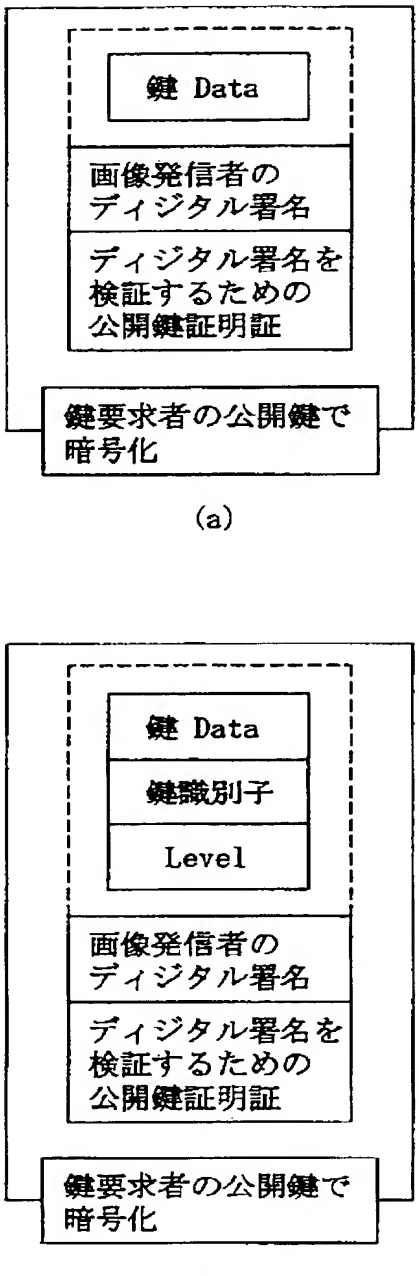
【図24】



【図25】



【図26】



【図27】